

FIG 1

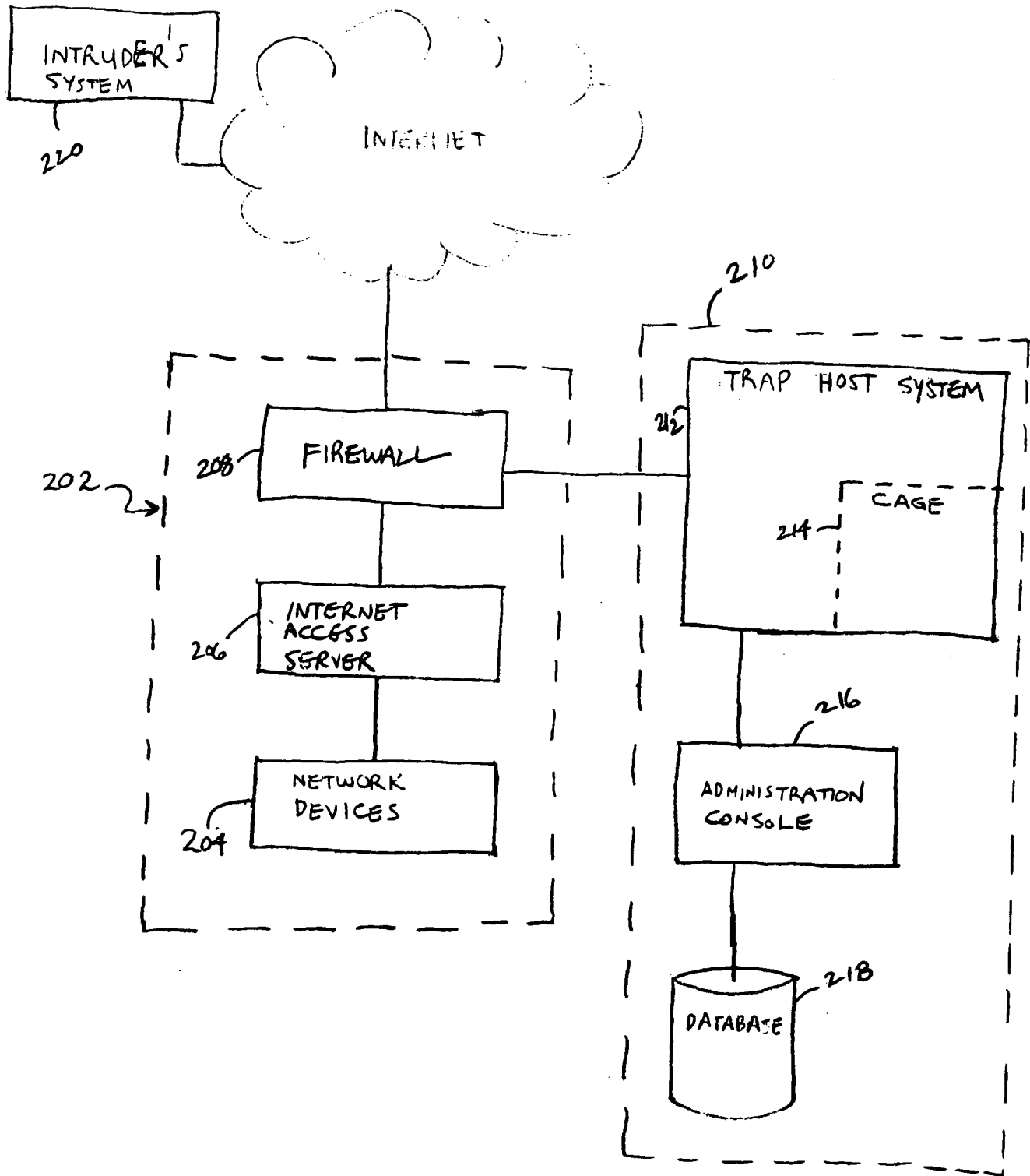


FIG. 2

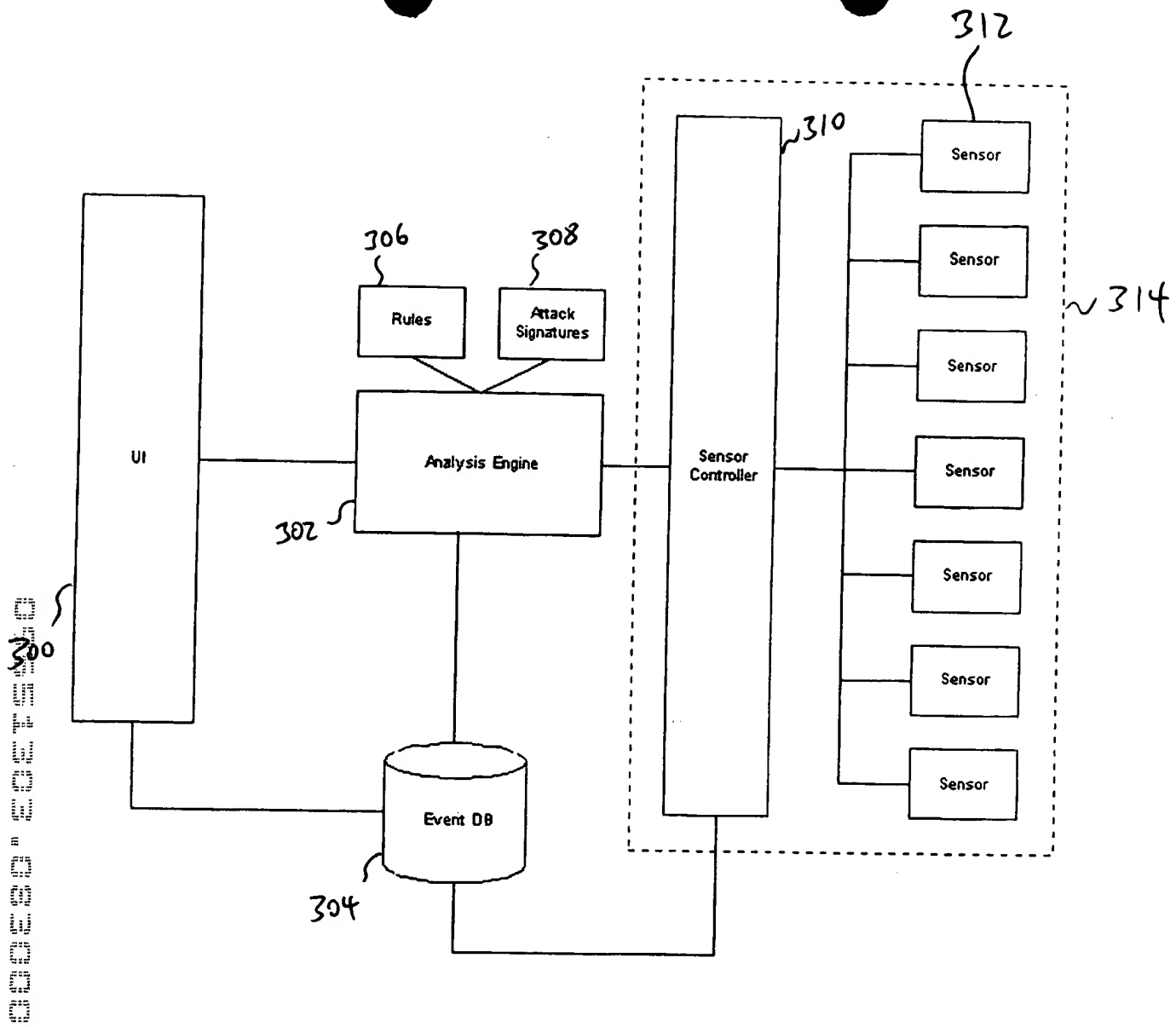


FIG. 3

Pattern of Remote Break-in

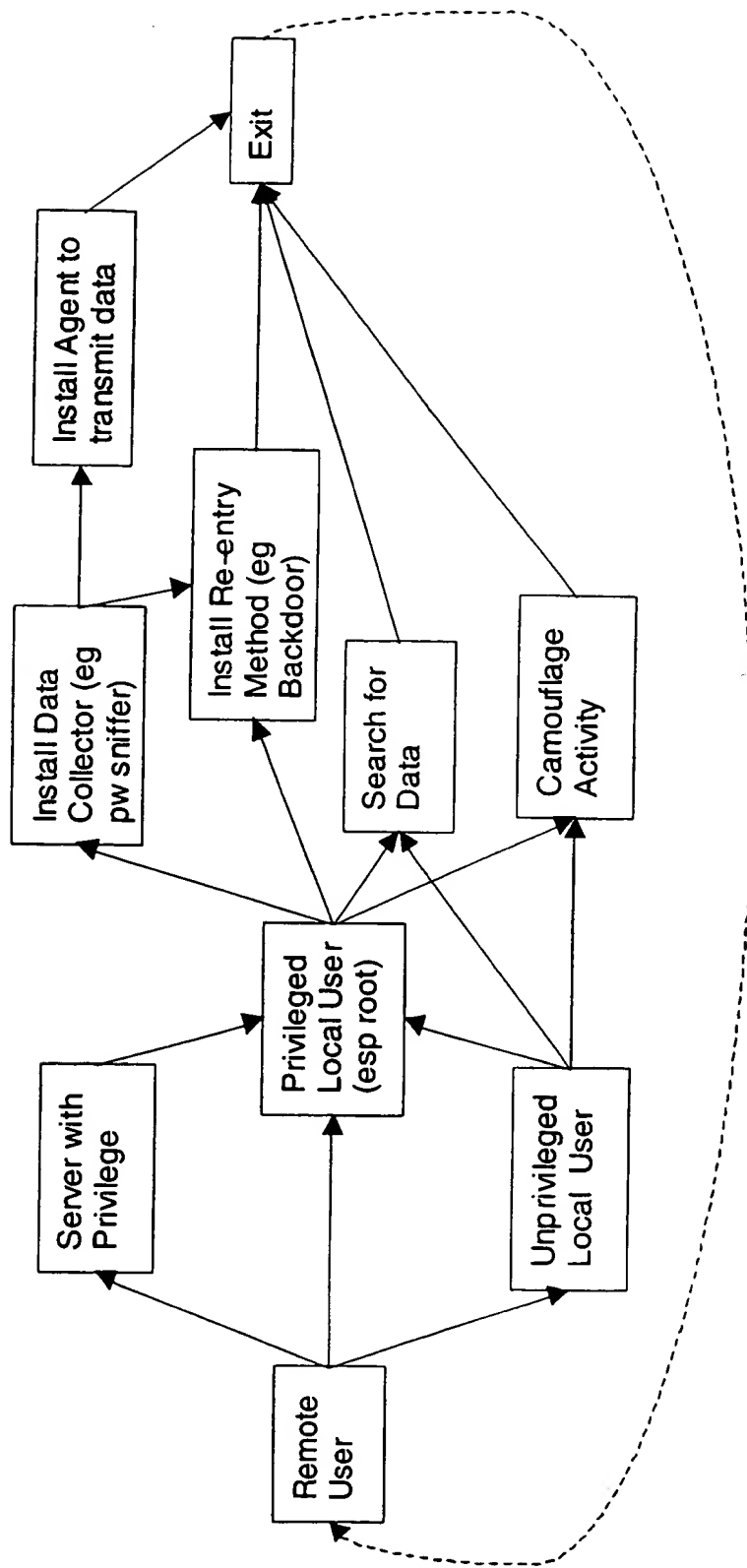


Fig 4

Timeline

2000-08-16 04:00:00]

04:55:41

Suspicious login – user jsmith ☒ from host snafu.com

Basis: (future) login at 2000-08-16 07:03:16

05:26:12

Suspicious login - rhost snafu.com ☒ from user tjones

Basis: suspicious login at 2000-08-16 04:55:41 ☒

Suspicious file - /home/tjones/eject-exp.uu - owner & modification time ☒

07:03:16

Suspicious login – user jsmith ☒ from host foobar.com

Basis: proximity of eject exploit (+00:01:07)

07:04:23

Probable exploit to root - eject

07:04:07

Suspicious file - /root/.rhosts - mtime

07:04:09

☒ Suspicious file - /etc/passwd - mtime

FIG. 5

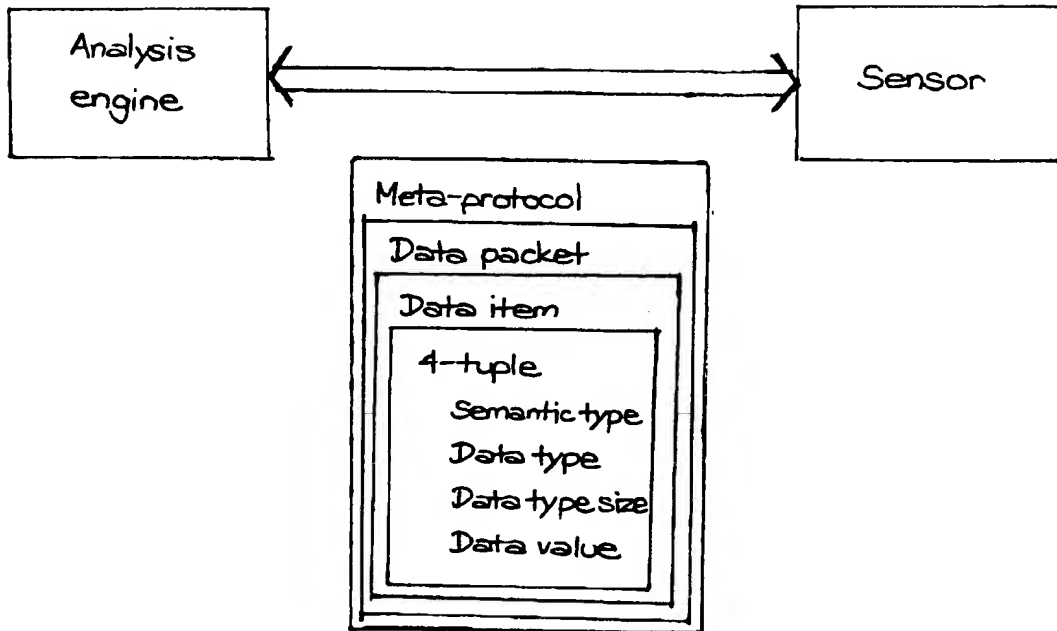


FIG. 7

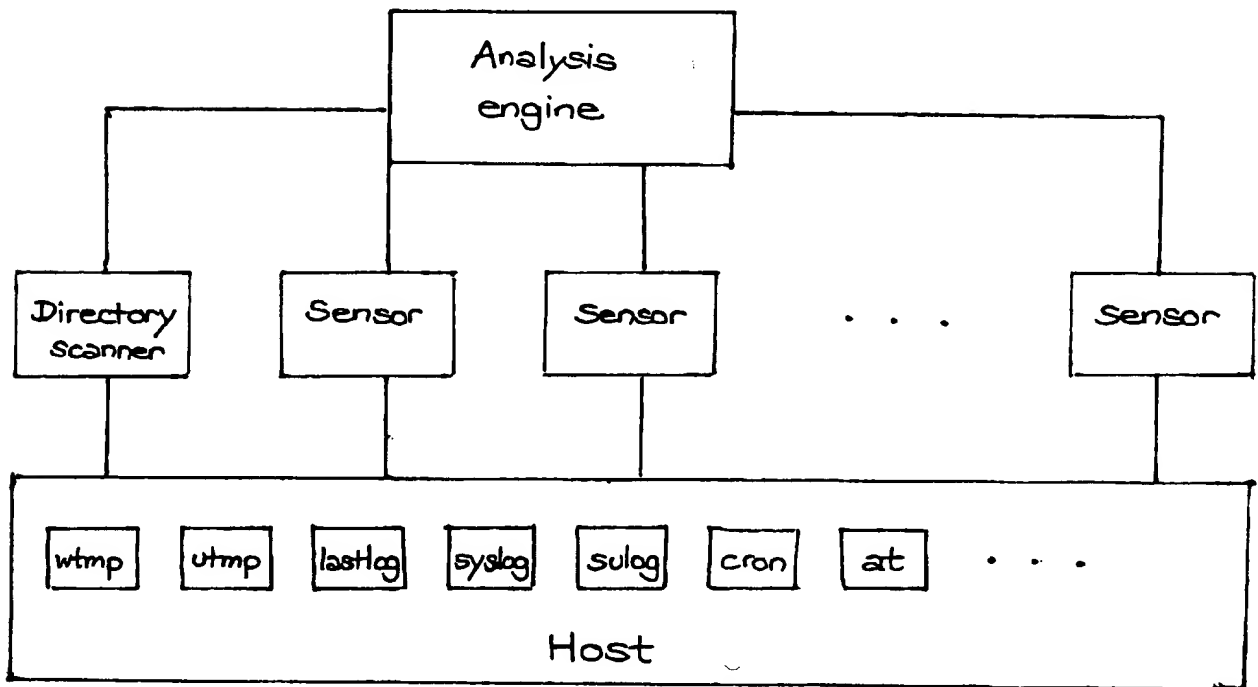


FIG. 8

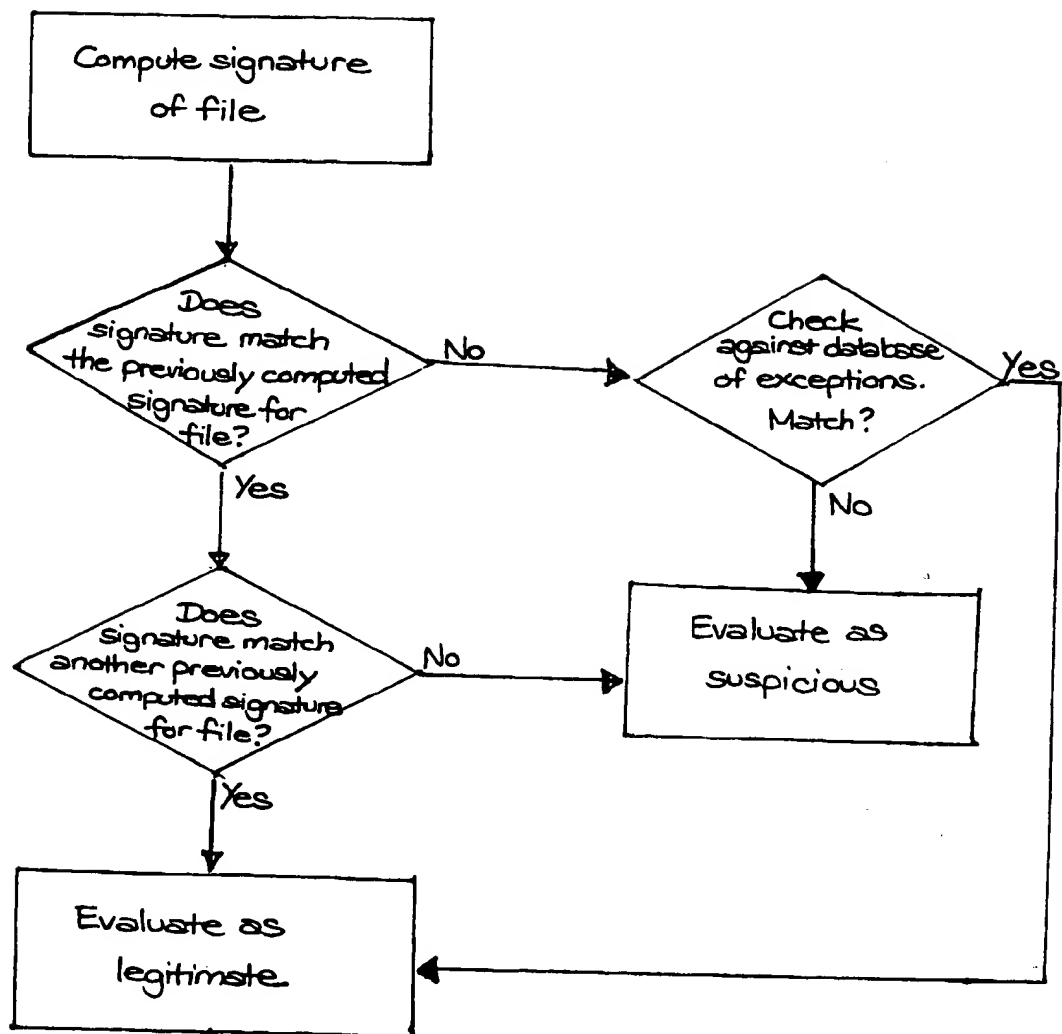


FIG. 9

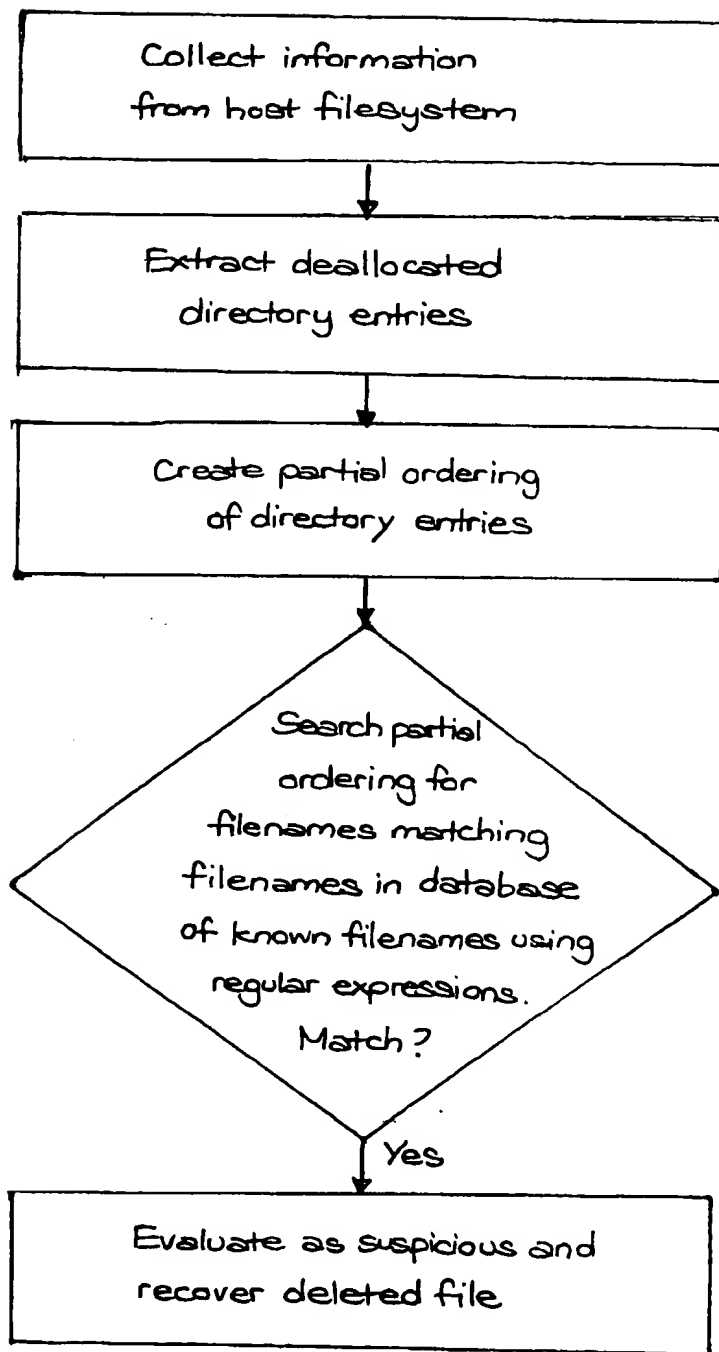


FIG. 10

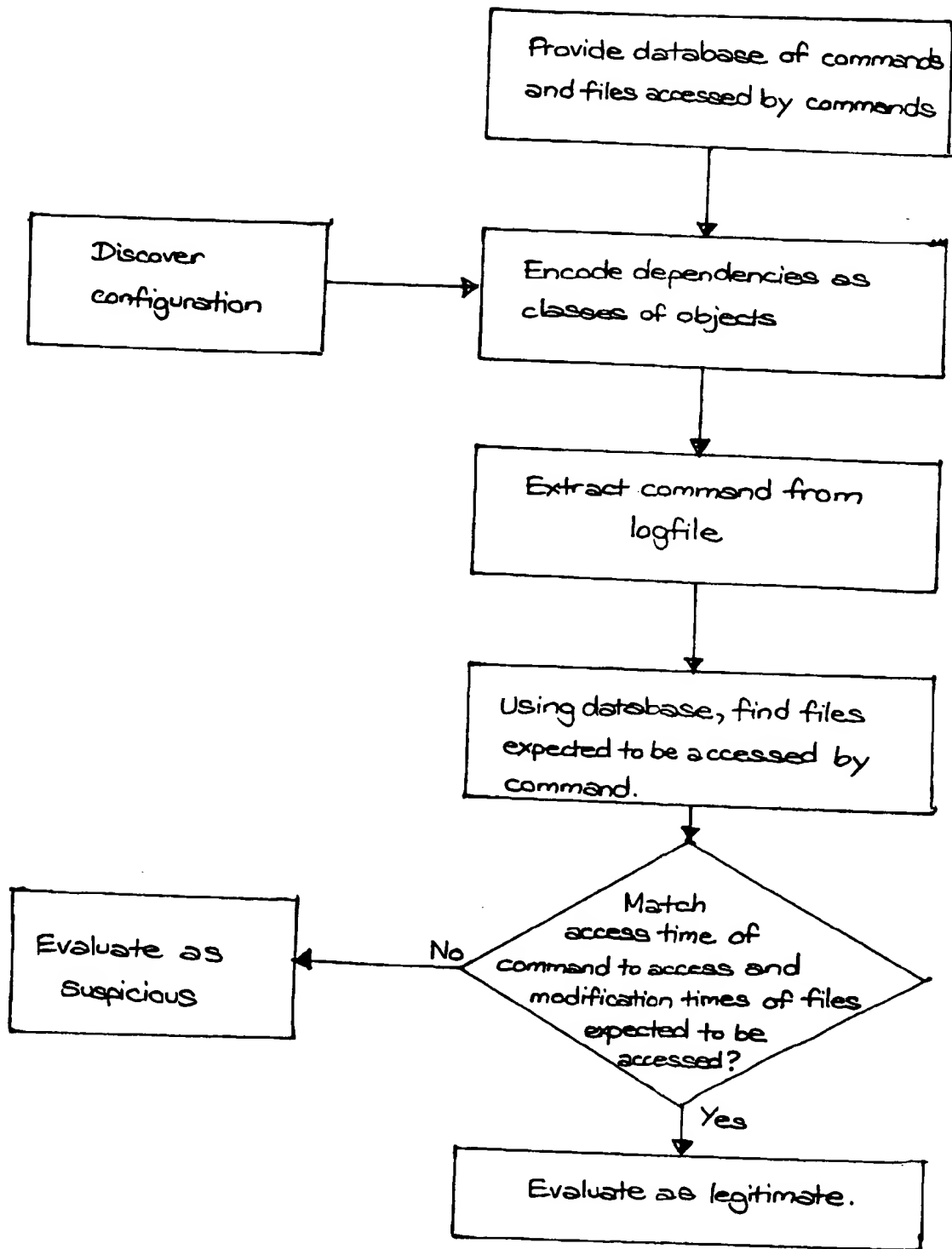


FIG. 11

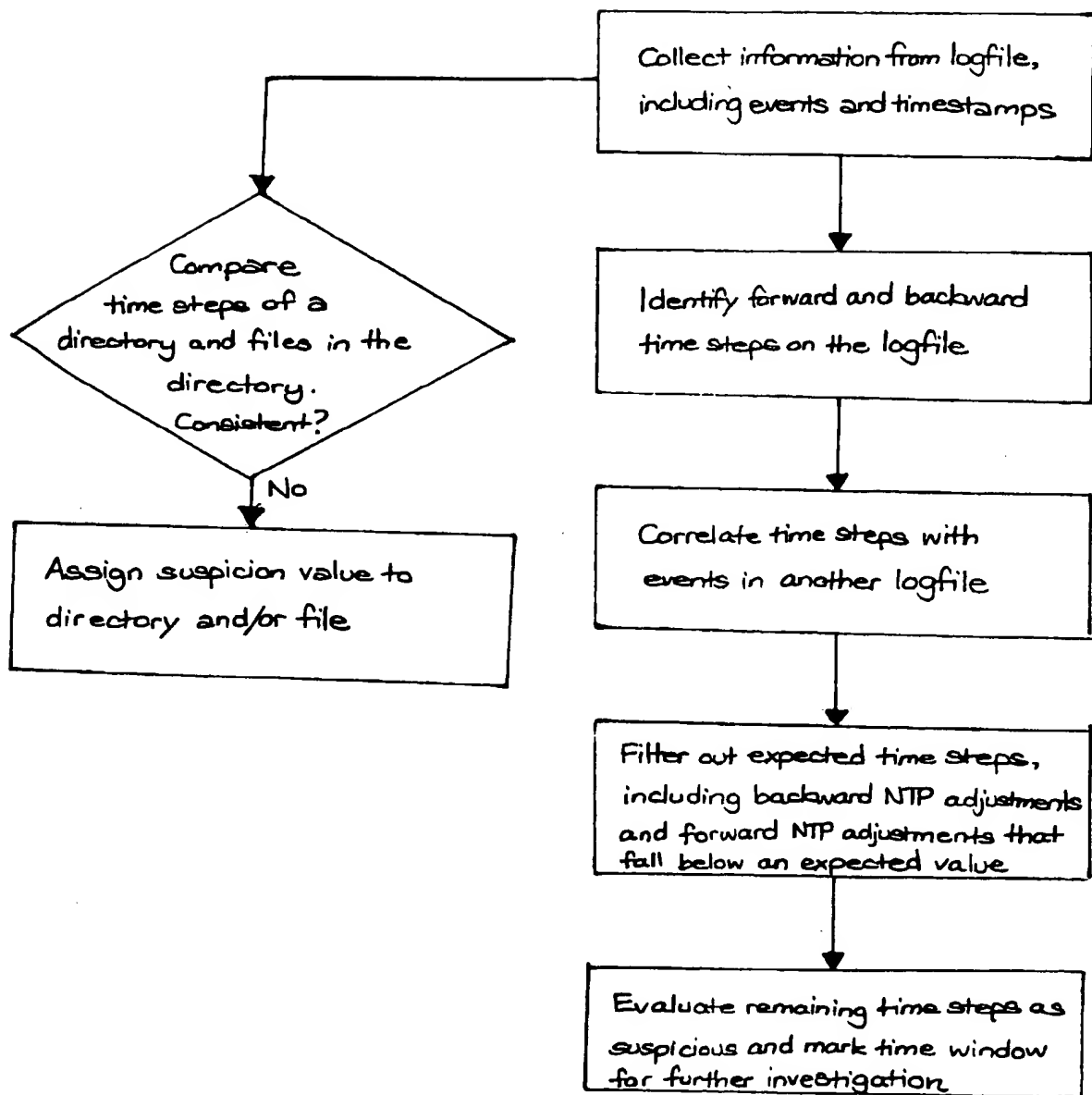


FIG. 12